

On minimal distance between q -ary bent functions

Vladimir N. Potapov
Sobolev Institute of Mathematics
Novosibirsk, Russia
vpotapov@math.nsc.ru

Abstract—The minimal Hamming distance between distinct p -ary bent functions of $2n$ variables is proved to be p^n for any prime p . It is shown that the number of p -ary bent functions at the distance p^n from the quadratic bent function is equal to $p^n(p^{n-1} + 1) \cdots (p+1)(p-1)$ as $p > 2$.

Keywords: bent function, Hamming distance.

I. INTRODUCTION

Bent functions is well known as Boolean functions with extremal nonlinear properties. Boolean bent function are intensively studied at present as they have numerous applications in cryptography, coding theory, and other areas. q -Ary generalizations of bent functions are an interesting mathematical subject as well (see [11]). In this paper we consider Hamming distances between different bent functions and properties of bent functions at minimal distance from each other. The Hamming distance between two discrete functions is the number of arguments where these functions are differ. In other words, the Hamming distance between two functions f and g is the cardinality of the support $\{x \in G \mid f(x) \neq g(x)\}$ of their difference.

II. FOURIER TRANSFORM ON FINITE ABELIAN GROUPS

Let G be a finite abelian group. Consider a vector space $V(G)$ consisting of functions $f : G \rightarrow \mathbb{C}$ with inner product

$$(f, g) = \sum_{x \in G} f(x) \overline{g(x)}.$$

A function $f : G \rightarrow \mathbb{C} \setminus \{0\}$ mapping the group to the non-zero complex numbers is called a character of G if it is a group homomorphism from G to \mathbb{C} , i.e. $\phi(x+y) = \phi(x)\phi(y)$ for each $x, y \in G$. The set of characters of an abelian group is an orthogonal basis of $V(G)$. If $G = Z_q^n$ then we can define characters of G by equation $\phi_z(x) = \xi^{\langle x, z \rangle}$, where $\xi = e^{2\pi i/q}$ and $\langle x, y \rangle = x_1 y_1 + \dots + x_n y_n \bmod q$ for each $z \in Z_q^n$. We may define the Fourier transform of a $f \in V(G)$ by the formula $\widehat{f}(z) = (f, \phi_z)/|G|^{1/2}$, i.e., $\widehat{f}(z)$ is the coefficients of the expansion of f in the basis of characters. Parseval's identity $(\widehat{f}, \widehat{f}) = \|f\|^2 = \|\widehat{f}\|^2$ and the Fourier inversion formula $(\widehat{f}(x)) = f(-x)$ hold. A proof of the following equation there can be found in [5].

Proposition 1: (uncertainty principle) For every $f \in V(G)$ the following inequality is true:

$$|\text{supp}(f)| |\text{supp}(\widehat{f})| \geq |G|. \quad (1)$$

If H is any subgroup of G , and we set f to be the characteristic function of H , then it is easy to see that $|\text{supp}(f)| = |H|$ and $|\text{supp}(\widehat{f})| = |G|/|H|$, so (1) is sharp. One can show that up to the symmetries of the Fourier transform (translation, modulation, and homogeneity) this is the only way in which (1) can be obeyed with equality.

If p is prime then Z_p^n can be considered as n -dimensional vector space over $GF(p)$.

Corollary 1: Let p be a prime number. An equation $|\text{supp}(f)| |\text{supp}(\widehat{f})| = p^n$ holds iff $f = c\phi_z\chi^\Gamma$, where $z \in G$, $c \in \mathbb{C}$ is a constant and χ^Γ is the characteristic function of an affine space Γ in Z_p^n .

The following equation can be found in [4] and [9].

Proposition 2: If p is a prime number and Γ is a linear subspace in Z_p^n , then it holds

$$\sum_{y \in \Gamma} \widehat{f}(y) = p^{\dim(\Gamma)-n/2} \sum_{x \in \Gamma^\perp} f(x).$$

Define the convolution of $f \in V(G)$ and $g \in V(G)$ by equation $f * g(z) = \sum_{x \in G} f(x)g(z-x)$. It is well known that

$$\widehat{f * g} = |G|^{1/2} \widehat{f} \cdot \widehat{g}. \quad (2)$$

We may define the Walsh–Hadamard transform of function $g : Z_q^n \rightarrow Z_q$ by the formula $W_g(z) = \xi^g(z)$.

III. BENT FUNCTIONS

A function $f : Z_q^n \rightarrow Z_q$ is called a q -ary bent function iff $|W_f(y)| = 1$ for each $y \in Z_q^n$ or $\widehat{\xi^f} \cdot \overline{\widehat{\xi^f}} = I$, where I is equal to 1 everywhere (see [3], [10]). By using (2) we can obtain that the definition of bent function is equivalent to the equation $\xi^f * \overline{\xi^f} = |G|\chi^{\{0\}}$. Then the matrix $B = (b_{z,y})$, where $b_{z,y} = \xi^{f(z+y)}$, is a generalized Hadamard matrix.

A bent function b is called regular iff there exists a function $b' : Z_q^n \rightarrow Z_q$ such that $\xi^{b'} = \overline{\xi^b}$. Then b' is a bent function as well. If q is a prime power and n is even, then each bent function is regular. We assume below that p is a prime number and n is even.

Proposition 3: 1) $\sum_{j=0}^{q-1} \xi^{kj} = 0$ as $k \neq 0 \bmod q$;
2) if q is a prime number then ξ is not a root of rational polynomial function of degree less than $q-1$.

Corollary 2: For any two p -ary bent functions b and b' , it holds $|\text{supp}(\xi^b - \xi^{b'})| = |\text{supp}(\xi^b - \overline{\xi^b})|$.

It is sufficient to show that there are $\frac{p-1}{2}$ different numbers of type $|\xi^i - \xi^j|^2$, ($i \neq j$), and these numbers are independent over \mathbb{Q} . Then from Proposition 1 and Corollary 1 we obtain

Corollary 3: The Hamming distance between two bent function on Z_p^n is not less than $p^{n/2}$. If it is equal to $p^{n/2}$, then the difference between these functions is equal to $c\chi^\Gamma$, where $c \in Z_p$ and Γ is an $n/2$ -dimensional affine subspace.

From Proposition 2 one can assume that the following statements is true.

Corollary 4: If a bent function $b : Z_p^n \rightarrow Z_p$ is an affine function on an affine subspace Γ , then $\dim \Gamma \leq n/2$.

Corollary 5: If a bent function $b : Z_p^n \rightarrow Z_p$ is an affine function on an $n/2$ -dimensional affine subspace, then there exist $p - 1$ bent function which differ from b only on this subspace.

Corollaries 3 – 5 was proved in [2] in the case of $p = 2$. In [8] it was found spectrum of potential small distances (less than the doubled minimum distance) between two bent functions in the binary case.

IV. QUADRATIC FORMS

A quadratic form $Q : (GF(q))^n \rightarrow GF(q)$ is called non-degenerate iff $\{x \in (GF(q))^n : \forall y \in (GF(q))^n Q(y + x) = Q(y)\} = \{0\}$. A linear subspace U in $(GF(q))^n$ is called totally isotropic iff $Q(U) = 0$. The maximal dimension of a totally isotropic subspace is often called the Witt index of the form. If $n = 2d$, then the maximal Witt index of a non-degenerate forms of degree n is equal to d . All non-degenerate forms with the maximal Witt index are equivalent. One of such quadratic forms is determined by the equation $Q_0(v_1, \dots, v_d, u_1, \dots, u_d) = v_1u_1 + \dots + v_du_d$. It is well known that Q_0 is a bent function from Maiorana–McFarland class (see [10]). The following proposition is proved, for example, in [1] (p.274, Lemma 9.4.1)).

Proposition 4: The number of the totally isotropic subspaces of Q_0 is equal to $\prod_{i=1}^d (q^{d-i} + 1)$.

It is easy to see that if Q_0 is an affine function on a some affine subspace, then it is an affine function on every coset. Moreover, if Q_0 is an affine function on a linear subspace of dimension d , then this subspace is isotropic (here we assume that $q > 2$). Thus Q_0 is an affine function on all cosets of totally isotropic subspaces and it is not affine on other linear subspaces of dimension d .

From Proposition 4 and Corollary 5 we can conclude that

Corollary 6: If p is a prime number and $p > 2$, then there are $p^d(p^{d-1} + 1) \cdots (p + 1)(p - 1)$ p -ary bent functions at the distance p^d from Q_0 .

In the binary case the analogous statement was proved in [6]. In [7] was established that this bound for the number of bent functions at the minimal distance is reached only for quadratic bent functions. It is natural to assume that this property of p -ary quadratic bent functions is true for any prime $p > 2$.

REFERENCES

- [1] Brouwer A. E., Cohen A. M., Neumaier A. Distance-Regular Graphs. New York: Springer-Verlag, 1989.
- [2] Carlet C. Two new classes of bent functions // Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Comput. Sci., no. 765, Berlin: Springer-Verlag, 1994. P. 77–101.

- [3] Kumar P. V., Scholtz R. A., Welch L. R. Generalized bent functions and their properties // J. Comb. Theory. Ser. A. 1985. V. 40, N 1. P. 90–107.
- [4] Sarkar P. Spectral domain analysis of correlation immune and resilient Boolean fuctions // Cryptology ePrint archive (<http://eprint.iacr.org/>), Report 2000/049, September 2000, 14 p.
- [5] Tao T. An uncertainty principle for cyclic groups of prime order // Math. Res. Lett. 2005. V. 12, N 1. P. 121–127.
- [6] Kolomeets N. A. Enumeration of the bent functions of least deviation from a quadratic bent function // J. Appl. Ind. Math., 2012, 6, No. 3, 306–317.
- [7] Kolomeets N. A. An upper bound for the number of bent functions at the distance 2^k from an arbitrary bent function in $2k$ variables // Prikl. Diskr. Mat., 2014, no. 3, 28–39 (in Russian)
- [8] Potapov V. N. Cardinality spectra of components of correlation immune functions, bent functions, perfect colorings, and codes // Problems of Information Transmission, 2012, 48:1, 47–55.
- [9] Tsfasman M. A., Vladuts, S. G. Algebraic geometric codes. Basic notations. Mathematical Surveys and Monographs 139. Providence, RI: American Mathematical Society. 2007.
- [10] Tokareva N. Bent functions. Results and applications to cryptography. Amsterdam: Elsevier. 2015.
- [11] Tokareva N. N. Generalizations of bent functions // Journal of Applied and Industrial Mathematics, 2011, 5:1, 110–129.